

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 04274058 A

(43) Date of publication of application: 30 . 09 . 92

(51) Int. Cl

G11B 20/12

G11B 7/00

G11B 20/10

(21) Application number: 03034439

(71) Applicant: OLYMPUS OPTICAL CO LTD

(22) Date of filing: 28 . 02 . 91

(72) Inventor: HORIGUCHI TOSHIO

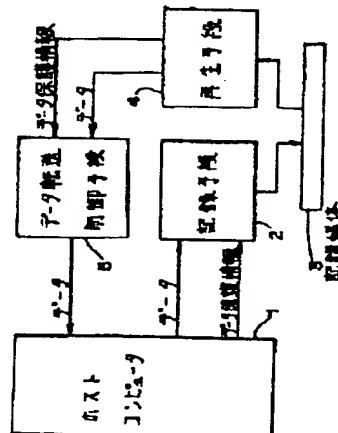
(54) INFORMATION RECORDING AND
REPRODUCING DEVICE

(57) Abstract:

PURPOSE: To provide the information recording and reproducing device which can prevent the reading of the information, such as personal information, to be kept secret with simple constitution.

CONSTITUTION: A recording means 2 which records the information on data protection to prohibit the inadvertent reading out of the data to be recorded on a recording medium 3 together with this data, a reproducing means 4 which reproduces the data recorded on the recording medium 3 and a data transfer control means 5 which permits the reading out of the data only when inputted password data coincides with the information on the data protection recorded on the recording medium 3 in the case of reproducing by this reproducing means 4 are provided. The protection of the data to be kept secret is thus assured by the simple constitution.

COPYRIGHT: (C)1992,JPO&Japio



(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平4-274058

(43) 公開日 平成4年(1992)9月30日

(51) Int.Cl.⁵
G 1 1 B 20/12
7/00
20/10

識別記号 庁内整理番号
9074-5D
E 9195-5D
H 7923-5D

F I

技術表示箇所

審査請求 未請求 請求項の数2(全8頁)

(21) 出願番号 特願平3-34439

(22) 出願日 平成3年(1991)2月28日

(71) 出願人 000000376

オリンパス光学工業株式会社
東京都渋谷区幡ヶ谷2丁目43番2号

(72) 発明者 堀口 敏夫

東京都渋谷区幡ヶ谷2丁目43番2号 オリ
ンパス光学工業株式会社内

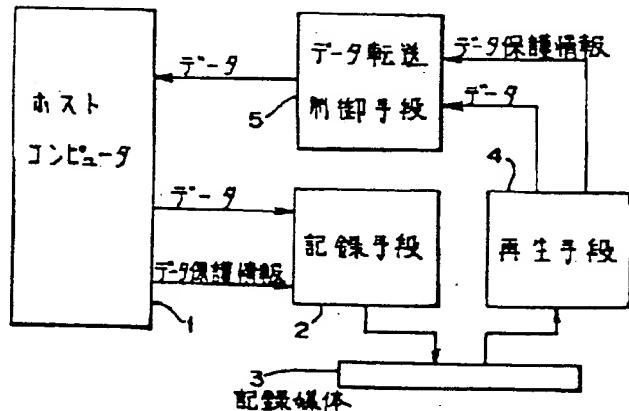
(74) 代理人 弁理士 伊藤 進

(54) 【発明の名称】 情報記録再生装置

(57) 【要約】

【目的】 簡単な構成で個人情報など秘密にすべき情報の読みとりを防止できる情報記録再生装置を提供することを目的とする。

【構成】 記録媒体3に記録されるべきデータと共に、そのデータが不注意に読み出されるのを禁止するデータ保護情報を記録する記録手段2と、記録媒体3に記録されたデータを再生する再生手段4と、この再生手段4により再生する場合、入力された暗証データが記録媒体3に記録されたデータ保護情報と一致する場合のみ、データの読み出しを許可するデータ転送制御手段5とを設けて、簡単な構成によって秘密にされるべきデータの保護を確保している。



1

2

【特許請求の範囲】

【請求項 1】 情報記録媒体に情報の記録及び再生を行う情報記録再生装置において、該情報記録再生装置の動作を制御するホストコンピュータと、該ホストコンピュータから転送される情報と共に、該情報の読み出しを禁止するための禁止情報を前記情報記録媒体に記録する記録手段と、前記情報記録媒体に記録された前記情報及び前記禁止情報を再生する再生手段と、該再生手段により再生された前記情報の前記ホストコンピュータへの転送を前記禁止情報に基づいて選択的に制御するデータ転送制御手段とを設けたことを特徴とする情報記録再生装置。

【請求項 2】 情報記録媒体に情報の記録及び再生を行う情報記録再生装置において、再生された情報を表示する表示手段と、前記情報記録媒体に情報を記録すると共に、前記情報の読み出しを禁止するための禁止情報を記録する記録手段と、前記情報記録媒体に記録された前記情報及び禁止情報を再生する再生手段と、前記再生された前記情報の前記表示手段への転送を制御するデータ転送制御手段とを設けたことを特徴とする情報記録再生装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は情報記録媒体に記録された秘密にされるべき情報の読み取りを禁止するデータ保護手段を設けた情報記録再生装置に関する。

【0002】

【従来技術】 情報記録媒体に情報を記録および／または再生を行う情報記録再生装置には、フロッピー・ディスクや磁気カード毎の磁気記録媒体、光ディスクや光カード等の光記録媒体がある。光記録媒体は光ディスクや光カード等、書換えはできないが、その記憶容量が大きいところから光ディスクは画像情報の記録、文書の保存等に、光カードは銀行用の預金通帳、携帯用の地図あるいは買物等に用いるプリペイドカード等としての広い応用範囲が考えられている。特に光カードは携帯性に優れることから、個人の健康管理情報等の個人のプライベートな情報を記録する用途も考えられている。従って、情報の暗号化等によって個人に特有な情報を他人の目から保護するための対策が検討されている。また、特開平1-286176号公報、特開昭62-192978号公報には、光カードや光磁気ディスクのセクタ内の一部に付加情報として本来の情報以外のデータを記録する方法が開示されている。

【0003】

【発明が解決しようとする問題点】 個人に関する秘密にされるべき情報を暗号化して記録し、再生時に暗号を復号する方法においては、暗号化／復号化を行う論理回路等のハード構成が必要となり、コストアップとなる問題点がある。また、ハードで構成しない場合においては、記録再生装置を制御するマイコン等を用いてプログラム

でソフトで行うこととなり、処理に時間がかかり、アクセスタイムの増大につながる恐れがある。

【0004】 特開平1-286176号公報とか特開昭62-192978号公報には、付加情報としてトラック番号、セクタ番号やディスクの識別情報を記録する例が開示されているにすぎず、情報の保護に関してはなんら記載されていない。

【0005】 この発明は、このような従来の問題点に着目してなされたもので、コストアップやアクセスタイムの増大を招くことなく、簡単な構成で個人情報など秘密が保持されるべき情報の保護を確保することのできる情報記録再生装置を提供することを目的とする。

【0006】

【問題点を解決する手段及び作用】 記録媒体に記録されるべきデータと共に、そのデータが不用意に読み出されるのを禁止するための暗証データとを記録する記録手段と、該記録手段により前記記録媒体に記録されたデータ及び暗証データとを再生する再生手段と、該再生手段により前記記録媒体から再生された暗証データが、再生時に入力された暗証データと対応する場合のみ、記録されたデータの読み取り／表示／転送を許可するデータ読み取り／表示／転送制御手段とを設けることにより、コストアップやアクセスタイムの増大を招くことなく、簡単な構成によって確実にデータの保護を行うようにしている。

【0007】

【実施例】 以下、図面を参照して本発明を具体的に説明する。図1ないし図7は本発明の第1実施例に係り、図1は第1実施例の概念的構成を示し、図2は光カードを示し、図3はトラックのフォーマットを示し、図4は図3の1セクタ分を示し、図5は第1実施例のブロック構成を示し、図6及び図7は記録時及び再生時の処理内容を示す。

【0008】 本発明の第1実施例の概要を図1に示す。ホストコンピュータ1は記録時にはデータと共にこのデータの読み取りを禁止してデータ保護するデータ保護情報を記録手段2に転送する。この記録手段2は記録媒体3に上記データ及びデータ保護情報を記録する。この記録媒体3に記録されたデータ及びデータ保護情報は再生手段4によって再生され、この再生されたデータ及びデータ保護情報はデータ転送制御手段5に転送される。このデータ転送制御手段5は、上記データ保護情報が再生の際に入力される入力情報に対応するものか否かの判断を行い、入力情報が対応するものであると判断した場合には再生したデータをホストコンピュータ1に転送し、対応するものでないと判断した場合にはホストコンピュータ1への転送を禁止して、データの読み取りから保護するようにしている。

【0009】 次に図2以降を参照して第1実施例を具体的に説明する。図2は第1実施例で使用する光カード1を示したものである。光カード1は、互いに平行な

複数のトラック 12 を有する光記録部 13 の両端部に、各トラックに対応してそのトラック情報を記録した ID 部 14A, 14B を設け、これら ID 部 14A, 14B 間をデータ部 15 としたものである。ID 部 14A, 14B は光カード 11 を製造する際に予めプリレコードしておく。

【0010】図 3 は図 2 のトラック 12 を拡大したもので、1 トラック内に 3 セクタの構成の場合のフォーマットの 1 例を示す。図 2 と番号の同じものは同じ機能のものを示す。21-1, 21-2, 21-3 はトラック 12 に記録されたセクタ・データ、22-1 はセクタ 21-1 と 21-2 間のギャップ、22-2 はセクタ 21-2 と 21-3 の間のギャップ、23 は ID 部 14A とセクタ・データ 21-1 との間のギャップ、24 は ID 部 14B とセクタ・データ 21-3 との間のギャップ、25, 26 はトラッキングを行うためのトラック・ガイドである。ギャップ 23, 24 は光カード 11 を定速で駆動する際の速度変動を吸収するために設けている。

【0011】図 4 で 1 セクタに記録されるデータの構成を示すように例えば各セクタの先頭部分には暗証情報などの付加データ 21-0 をそれぞれ記録するようにしている。図 4 に示す 1 セクタのデータの構成は、データ数 256 バイトと、このデータに対して暗証情報となる付加データ 8 バイトの計 264 バイトを積符号となるようにエラー訂正用のリードソロモン符号（以下 RS 符号）を付加して C2 符号を (16, 12) RS 符号、C1 符号を (26, 22) RS 符号としたものである。光カードへの記録時には、このように符号化したデータブロックを行方向にバイト毎に順次読み出し、シリアルデータに変換して 1 セクタ内に記録する。付加情報のデータの構成は、暗証番号 4 バイト、エラー訂正用の C3 符号を (8, 4) RS 符号としたものである。

【0012】図 5 は、光カード読出し／書き込み装置内にあって光カード 11 からのデータの読出し／書き込み動作を制御するコントローラ、つまり第 1 実施例の情報記録再生装置の主要部の構成のブロック図を示したものである。光カードに対向配置された光学ヘッド 31 内の光検出器 (PD) 32 の出力は、復調回路 33 に入力され、エラー訂正前のデータとしてバイト単位で復調され、第 1 DMA 回路 34 を介して一時的にデータを格納する第 1 バッファ 35 に格納される。この第 1 DMA 回路 34 は、読出し時（再生時）には、復調されたデータをこのコントローラ全体の動作を制御する CPU 36 を経ることなく、第 1 バッファ 35 に転送し、書き込み時（記録時）には、第 1 バッファ 35 に格納されたデータを変調回路 37 に転送する。この変調回路 37 は、記録時に第 1 DMA 回路 34 を介して転送されるデータをシリアルの書き込みデータに変換し、光学ヘッド 31 内のレーザダイオード 38 の発光を書き込みデータに応じて発光させる変調動作を行う。

【0013】上記第 1 バッファ 35 は、読出し時には第 1 DMA 回路 34 を介して転送された復調データを EDAC 回路 (Error Detection and Correction Circuit) 39 に転送し、この EDAC 回路 39 によってエラー検出及びエラー訂正を行わせる。又、この第 1 バッファ 35 は書き込み時には EDAC 回路 39 によって、エラー訂正用符号が付加されたデータ（後述するホストコンピュータ 42 から送られるデータ）を第 1 DMA 回路 34 を介して変調回路 37 に転送する。

【0014】上記 EDAC 回路 39 によってエラー訂正されたデータは第 2 バッファ 40 に格納され、この第 2 バッファ 40 は第 2 DMA 回路 41 により、ホストコンピュータ 42 との間でデータの転送が行われる。読出し時には、第 2 バッファ 40 に格納されたエリア内の暗証エリアのデータがこのデータを保護すべきデータであるか否かを CPU 36 が判断し、保護を必要としないデータの場合には第 2 DMA 回路 41 の DMA 機能を許可し、保護を必要とするデータの場合には読出し時にキー入力手段 43 によって入力された暗証データと一致するか否かの判断を行い、一致した場合のみ第 2 DMA 回路 41 の DMA 動作を許可し、そうでない場合にはその DMA 動作を禁止する。

【0015】従って、DMA 動作が許可された場合には第 2 DMA 回路 41 によってホストコンピュータ 42 にデータが転送されることになり、このデータが転送されるとホストコンピュータ 42 は例えば表示手段 44 によって読出されたデータを表示する。一方、第 2 DMA 回路 41 による転送が禁止された場合にはデータがホストコンピュータ 42 側に転送されず、この場合にはホストコンピュータ 42 は例えば表示手段 44 にデータ読出しエラーと表示し、秘密が保持されるべきデータが不用意に読み出されるのを防止するようになっている。

【0016】CPU 36 は、ホストコンピュータ 42 から第 2 DMA 回路 41 を介して転送された（キー入力手段 43 によって入力された）暗証データを、この CPU 36 内のメモリ 36a に記憶しておくことによって、第 2 バッファ 40 の暗証エリア内のデータ（つまり、暗証番号データ）と一致しているか否かの判断を行う。記録時にはキー入力手段 43 によって入力された暗証データは、一旦このメモリ 36a 内に格納され、ホストコンピュータ 42 から第 2 DMA 回路 41 を介して第 2 バッファ 40 に格納される本来のデータに対し、第 2 バッファ 40 内に予め設けた暗証エリアの位置にこの暗証データを格納し、その後 EDAC 回路 39 により、エラー訂正用の符号が付加される。そして、このエラー訂正用符号が付加されたデータは第 1 バッファ 35 に格納され、第 1 DMA 回路 34、変調回路 37 を介してレーザダイオード 38 が発光制御され、光カードに暗証番号を付して記録し、その際暗証番号は例えば各セクタの先頭位置に記録されるようになっている。

【0017】上記EDAC回路39は暗証番号に対しては二重にエラー訂正を行うように符号化しているので、暗証番号単独でも信頼性は高い。次に図6を参照して光カード上のセクタに暗証番号を付加して記録する動作を説明する。この記録動作がスタートしたならば、記録されるデータを秘密にすべきものか否かに応じて暗証番号をキー入力手段43によりキー入力する(ステップS1)。つまり、読み取りを防止するべきデータの場合には、例えばこのデータが記録される光カードに応じて設けた暗証番号を入力し、そうでない場合には暗証番号としない方を選択したり、単にリターンキーを押して暗証番号を入力しない。

【0018】すると、ホストコンピュータ42は有効なキー入力があったか否かを判断し(ステップS2)、有効なキー入力であった場合にはステップS3aに示すように、このホストコンピュータ42からの暗証セットコマンドにより暗証番号をCPU36の内部のメモリ36aにセットし、有効なキー入力が行われなかった場合にはステップS3bに示すように、ホストコンピュータ42からのセットコマンドにより秘密にする必要のないデータであることを表す(さらに暗証番号と同じバイト数のデータ)例えばFFF FFFF FFHをセットする(Hは16進であることを表す)。

【0019】つまり暗証番号としない場合には4バイトの所定のデータFFF FFFF FFHとし、一方暗証番号の場合には同じく4バイトのデータでFFF FFFF FFH以外のデータにする。上記ステップS3a又はS3bによるデータのセットが終了すると、次に記録を行うコマンドと例えば1セクタ分のデータとがホストコンピュータ42からこのコントローラに転送され、第2DMA回路41を介して第2バッファ40に1セクタ分のデータが転送される(ステップS4)。

【0020】次に、CPU36は、暗証セットコマンドで受け取った暗証番号(有効な暗証番号でない場合にはFFF FFFF FFH)4バイトを第2バッファ40内の暗証エリアに転送する(ステップS5)。次にEDAC回路39を起動し、第2バッファ40内のデータ(つまり光カードに記録されるべき通常のデータ及びそのデータを保護すべきか否かを表す暗証番号または非暗証番号)に対してエラー訂正用の符号を発生させ、その結果を第1バッファ35内に格納する(ステップS6)。この第1バッファ35に格納する場合、データ全体にインターリープをかけても良い(この場合には、図3に示すように1セクタの先頭部分に暗証番号などの付加データが書き込まれるものとは異なる)。

【0021】次に、光学ヘッド31に記録を行うトラックにシークさせ(ステップS7)、第1DMA回路34を介して、第1バッファ35内のデータを変調回路37に転送し、この変調回路37によりこのバッファ35から送られるデータを光カード上に記録するデータに変調

してレーザダイオード38の発光を制御して光カードへのデータ記録を行う(ステップS8)。このデータ記録により、図3のようにデータが記録されることになり、記録動作を終了する。実際には、この記録の後、このデータを再生して光カード上に記録されたデータが再生により復元されたデータと一致するか否かのペリファイ動作を行うことが多い。

【0022】次に上記のような記録動作によって、光カード上に記録されたデータを読出す再生動作を図7を参考して以下に説明する。記録動作と同様に、最初にキー入力手段43により暗証番号をキー入力する(ステップS11)。このキー入力により暗証番号4バイトがホストコンピュータ42からのセットコマンドにより、入力された暗証番号をCPU36内のメモリ36aにセットする(ステップS12)。データを読出すためには、この暗証番号は記録時にセットしたものと同じものであることが必要になる。

【0023】次にCPU36はホストコンピュータ42からの読み出しコマンドを受け取り、読み出しを行う目的ト20ラックに光学ヘッド31をシークさせる(ステップS13)。そして、光検出器32で検出された光カードからの読み出しデータは復調回路33で復調され、DMA回路34の動作によって読み出したデータを第1バッファ35に格納する(ステップS14)。次に、EDAC回路39の動作によって第1バッファ35内のデータに対してエラー検出及び訂正動作を行い、その結果を第2バッファ40に格納する(ステップS15)。(記録動作時にインターリープをかけた場合には、ここでデ・インターリープさせる。)この結果、第2バッファ40にはエラーデータを施したデータと暗証番号が格納されている。

【0024】次に、CPU36は、第2バッファ40内の暗証エリア内の暗証番号を読み取り、この暗証番号がプロテクトの必要のないデータであるか否かの判断、つまりこの暗証番号がFFF FFFF FFHであるか否かの判断を行う(ステップS16)。この判断でプロテクトの必要のないデータであると、次のステップS17により暗証番号を除いた本来のデータがホストコンピュータ42に転送される(ホストコンピュータ42は転送されたデータを例えば表示手段44に表示する。)。

【0025】一方、上記ステップS16の判断が否の場合には、暗証セットコマンドで予めセットされた暗証データと同じであるか否かの判断が行われる(ステップS18)。この判断により暗証エリア内のデータが暗証セットコマンドによりセットされた暗証データと一致しない場合には、ホストコンピュータ42にデータ読み出しエラーを報告し(ステップS19)、例えば表示手段44にはリードエラーと表示してデータの読み出しに対するプロテクトを確保する。

【0026】一方、上記ステップS18の判断において

て、暗証エリア内のデータが（暗証セットコマンドによりセットされ、）この光カードに対して実際に使用されている暗証データと一致している場合には、暗証番号を知っている者とみなされるので、この場合にはステップ S 17 に示すようにホストコンピュータ 4 2 にデータを転送する。

【0027】このようにすることによって、プロテクトの必要なデータに対して、暗証番号を知らない他人が読出そうとする場合には最大 2³² とおりの試行が必要となり、プロテクトを破ってデータを読出すことは不可能に近い。このようにして書込むデータにプロテクトをかける必要がある場合にはデータ記録時に入力される暗証番号をデータと共に記録し、一方書込むデータをプロテクトする必要のない場合には、データ記録時に暗証番号として使用されるデータ以外のデータ F F F F F F F F H を自動的に記録するようにし、読出し時には暗証エリアのデータが F F F F F F F F F H である場合には、プロテクトが不要とみなして読出したデータをホストコンピュータ 4 2 に転送するようにしている。また、ここでは暗証を 4 バイトのデータとしたが、暗証に付加するエラー訂正用のコード部分も暗証として暗証を 8 バイト長とすることによってさらにセキュリティを上げることができる。

【0028】尚、暗証番号としては、光カード毎に異なるように設定しても良いし、1人のユーザには1つの暗証番号を割り当てるようにしても良い。又、1つの光カードに対しての暗証番号として、トラック番号とかセクタ番号を含めるようにしても良く、トラックとかセクタ毎に異なる暗証番号にしても良い（4 バイト分の暗証データの一部をトラック番号とかセクタ番号に割り当てても良い）。

【0029】次に本発明の第2実施例を説明する。第1実施例では暗証番号や演算結果が一致しない場合に、暗証番号や演算結果を変更して再試行を容易に行うことができるため、偶然入力キーの番号が一致してセキュリティがなくなる恐れがゼロとは言えない。第2実施例では、再試行を容易には行えないようにした例を示す。

【0030】光カード記録再生装置の動作モードとして、以下の2つを用意する。まず、第1モードとして、データ読出し時に暗証番号を使用しないモードを用意する。このモード中では、第1実施例で説明した暗証番号のセットコマンドは使用できない（イリーガルコマンドとする。）ようにし、暗証番号が F F F F F F F F H の時のみ、データをホストコンピュータ 4 2 に転送する。従って、もし暗証番号が F F F F F F F F H でない場合には、このモードにいる限りは永久に読出せないことになる。

【0031】第2モードとしては、データ読出し時に暗証番号を使用するモードとする。このモード中では第1実施例で述べたような処理を行って読出しデータのプロ

テクトをかける。このモードでは、暗証番号のセットコマンドは有効である。この実施例ではモードセットコマンドによって、第1のモードから第2のモードに切換えられるようになっている。

【0032】上述した2つのモードは、光カード記録再生装置の電源ON時に最初に送られるホストコンピュータ 4 2 から C P U 3 6 へのモードセットコマンドによってどちらのモードとなるかを決定し、いったんどちらかのモードに入ったならば、電源をOFFするまで他のモードには移行できないようにする。そして、この電源ON時に、モードセットコマンドが入力されないと、第1のモードに設定されるようになっている。このように構成することによって、ユーザーに対するアクセスのキーは暗証番号と装置の動作モードの2つとなり、第1実施例に比べてより高いセキュリティを確保することができる。

【0033】次に本発明の第3実施例を説明する。図8は本発明の第3実施例の光カード記録再生装置の概略の構成を示す。この記録再生装置は、スタンドアローン型のものである。つまり、図1のホストコンピュータ 1 を有しないで、コントローラ 5 2 からデータ及びデータ保護情報を記録手段 2 に転送する。又、データ転送制御手段 5 は表示手段 5 3 にデータの表示を行うか否かを制御するようになっている。その他の構成は図1と同様であり、同符号を付して、その説明を省略する。

【0034】次に、図9を用いてより具体的な構成を示す。この記録再生装置 5 1 は、図5に示す装置において、ホストコンピュータ 4 2 がなく、第2バッファ 4 0 は C P U 3 6 とデータを転送できるようにしてある。又、この実施例では、キー入力手段 4 3 及び表示手段 4 4 は、C P U 3 6 と接続され、キー入力手段 4 3 から入力される暗証番号を C P U 3 6 内部または外部のメモリ 3 6 a' に記憶し、再生により光カードから読出した際の第2バッファ 4 0 の暗証エリア内の暗証番号と一致するか否かの判断を行うことにより、表示手段 4 4 に表示するか否かを制御する。

【0035】つまり、第1実施例では、再生時において入力された暗証番号が暗証エリア内の暗証データと一致するか否かに応じて、ホストコンピュータ 4 2 側にデータを転送するか否かを制御していたが、この第3実施例では、表示手段 4 4 へ表示するか否かを制御するようになっている。そして、入力された暗証番号が暗証データと一致する場合のみ表示手段 4 4 にデータの表示を行い、それ以外では表示を禁止して、データのプロテクトを確保するようにしている（但し、データがプロテクトされている場合）。その他の構成は図5に示すものと同様であり、同一構成要素は同符号を付してその説明を省略する。

【0036】この第3実施例の作用効果は第1実施例とほぼ同様のものとなる。尚、上記表示手段 4 4 と共に、

プリンタなどのデータ出力手段を有する場合には、表示手段4-4での表示が禁止される場合には同時に、データ出力手段へのデータ転送なども禁止する。

【0037】尚、例えば1つの光カードに対して1つの暗証番号を共通に設定し、記録時に入力されるその暗証番号に対し、その暗証番号と共にデータが実際に記録されるトラックあるいはセクタ番号と加減乗除などの一定の演算を施した演算結果の（例えばその4バイト分のみの）暗証データを本来のデータとインタリープなどで実際に記録するようにしても良い。この場合には、再生時には逆演算などして、記録時と同じ暗証番号が入力された場合には、同様に対処できるようにする。

【0038】このようにすると、この光カードを第1実施例の装置とは異なる構成（または機能）の一般的な再生装置を用いて、本来のデータ分を読み取ろうとしてもその演算規則が分からないと、読み取ることができず、その秘匿性を確保できる。

【0039】尚、記録媒体に記録される暗証番号として、例えばエラー訂正用の符号を付けないで行い、再生時には一定のゲート期間内にこの暗証番号が読み出されるようにして、再生時に入力される暗証番号と一致するか否かをパターンなどで判断してその判断結果に応じて例えばこの後に再生されるデータの読み取り動作を停止ないしは禁止するようにしても良い。尚、上述した各実施例を部分的に組合せて異なる実施例を構成することもできる。

【0040】

【発明の効果】以上述べたように本発明によれば、記録媒体に記録されるべきデータと共に、そのデータが不注意に読み出されるのを禁止する暗証データなどの付加データとを記録し、再生時には、入力された暗証データが記録媒体に記録された暗証データと一致または対応する場合のみ、データの読み出しを許可するようにしているので、簡単な構成によってデータのプロテクトを確保できる。

【図面の簡単な説明】

【図1】本発明の第1実施例の概念的構成図。

【図2】第1実施例に用いられる光カードの説明図。

【図3】光カードのトラックの一部を拡大して示す説明図。

【図4】図3の1セクタを拡大して示す説明図。

【図5】第1実施例の主要部の構成を示すブロック図。

【図6】第1実施例の記録時の動作内容を示すフローチャート。

10 【図7】第1実施例の再生時の動作内容を示すフローチャート。

【図8】本発明の第3実施例の概念的構成図。

【図9】第3実施例の概略の構成を示すブロック図。

【符号の説明】

1 ……ホストコンピュータ

2 ……記録手段

3 ……記録媒体

4 ……再生手段

5 ……データ転送制御手段

20 1 1 ……光カード

1 2 ……トラック

1 3 ……光記録部

3 1 ……光学ヘッド

3 3 ……復調回路

3 4 ……第1DMA回路

3 5 ……第1バッファ

3 6 ……CPU

3 7 ……変調回路

3 8 ……レーザダイオード

3 9 ……EDAC回路

4 0 ……第2バッファ

4 1 ……第2DMA回路

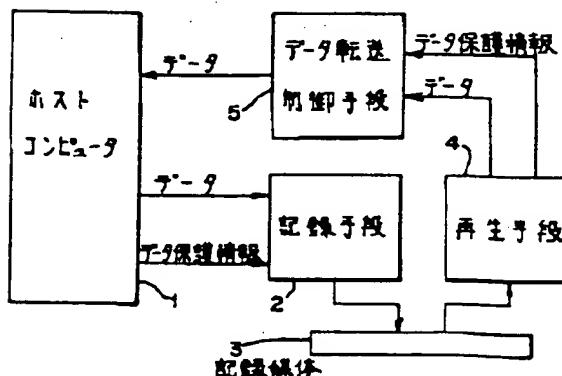
4 2 ……ホストコンピュータ

4 3 ……キー入力手段

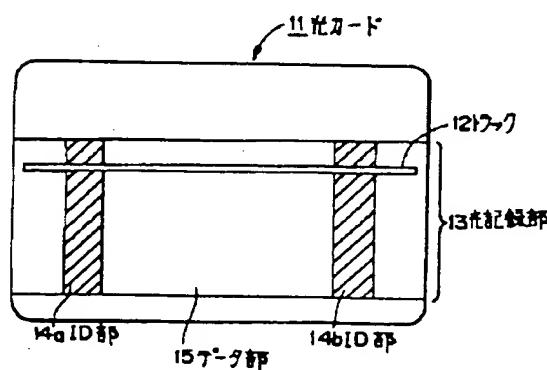
4 4 ……表示手段

30 30 1 1 ……光カード
1 2 ……トラック
1 3 ……光記録部
3 1 ……光学ヘッド
3 3 ……復調回路
3 4 ……第1DMA回路
3 5 ……第1バッファ
3 6 ……CPU
3 7 ……変調回路
3 8 ……レーザダイオード
3 9 ……EDAC回路
4 0 ……第2バッファ
4 1 ……第2DMA回路
4 2 ……ホストコンピュータ
4 3 ……キー入力手段
4 4 ……表示手段

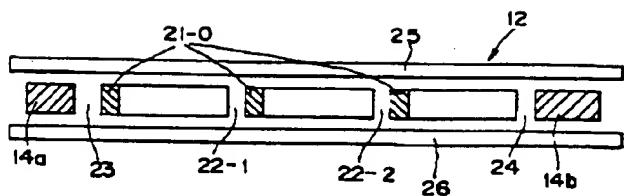
【図1】



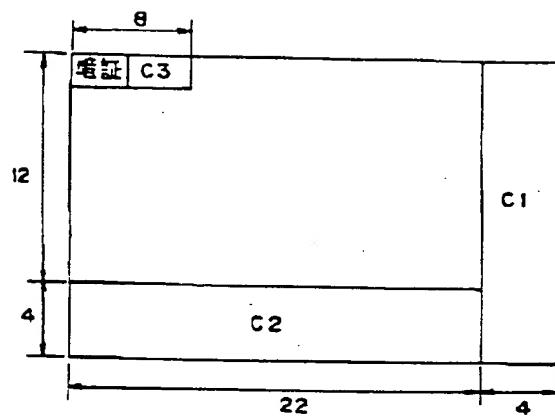
【図2】



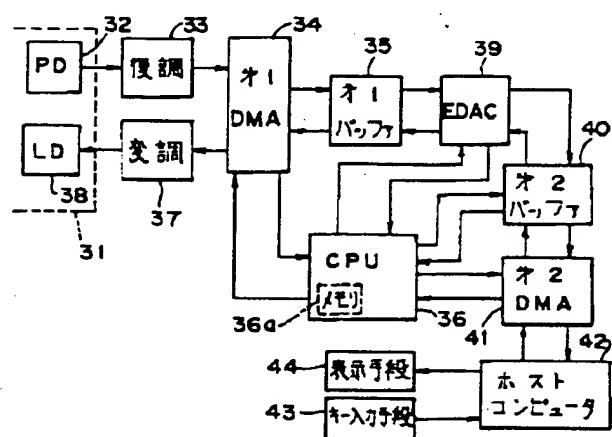
【図3】



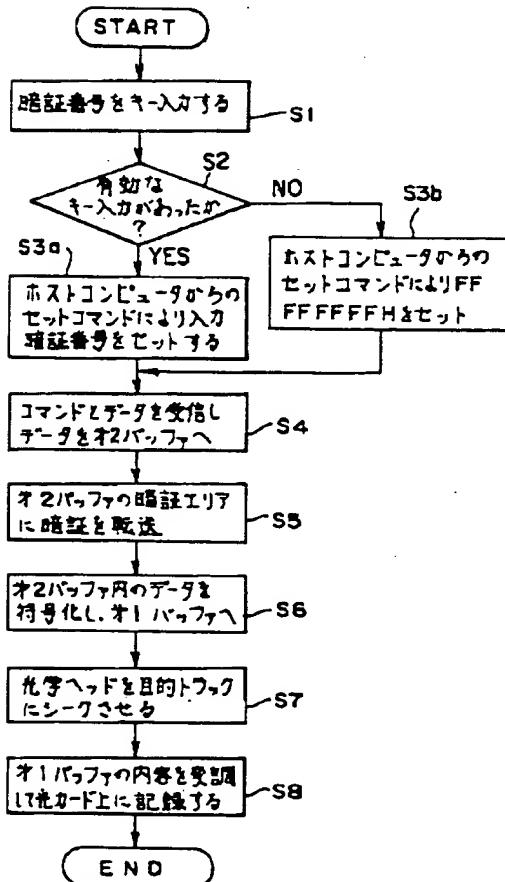
【図4】



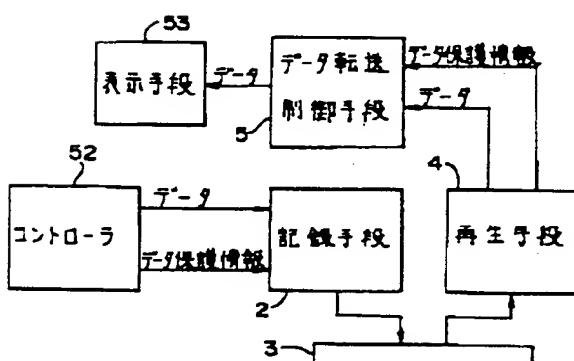
【図5】



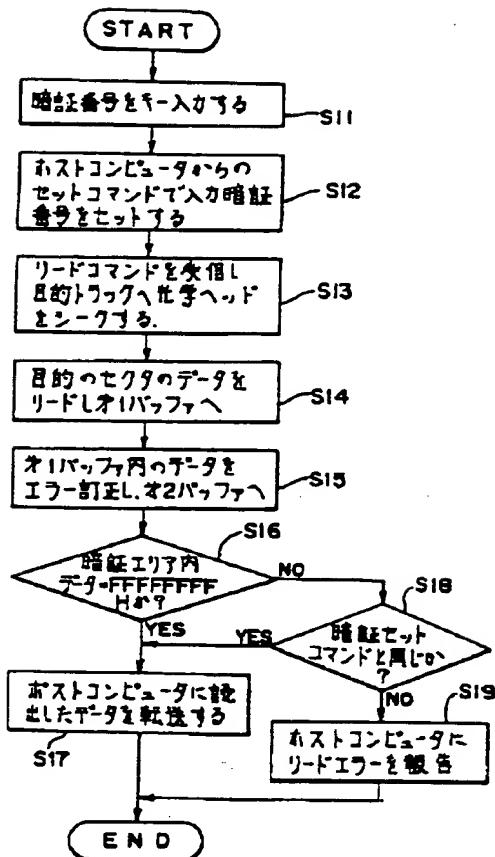
【図6】



【図8】



【図7】



【図9】

